REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* **18-05-2004**	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

CHANGING THE LINES IN THE COLORING BOOK

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

CDR LEWIS T. BOOKER, JR., JAGC, USN

Paper Advisor (if Any): N/A

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Operational Commanders may find themselves hamstrung by definitions rooted too firmly in the past. The ability to affect a nation's "life" and "well-being" through nonkinetic electronic means is a real and potent threat; therefore, the Operational Commander must advance the thinking to allow self-defensive actions in light of those threats, and not simply the "punch in the nose" required under existing State practice.

The Operational Commander must think of "hostile act," "hostile intent," and "lethal fires" in a new environment, that of the electronic attack against ideals, and must propose to the Strategic level of command a rationale for departing from existing State practice. This paper gives some thoughts in those regards, reviewing existing law, examining potential future threats and means for further investigating them, and then setting out a good-faith basis for modification or extension of existing law.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**THIS PAGE** UNCLASSIFIED		**44**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

`

NAVAL WAR COLLEGE
Newport, RI

CHANGING THE LINES IN THE COLORING BOOK

By

Lewis T. Booker, Jr.
CDR, JAGC, USN

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College, the Department of the Navy, the Department of Defense, or any other agency of the Executive Branch of the United States Government.

LEWIS T. BOOKER, JR.
18 May 2004

`

TABLE OF CONTENTS

ABSTRACT

Operational Commanders may find themselves hamstrung by definitions rooted too firmly in the past. The ability to affect a nation's "life" and "well-being" through nonkinetic electronic means is a real and potent threat; therefore, the Operational Commander must advance the thinking to allow self-defensive actions in light of those threats, and not simply the "punch in the nose" required under existing State practice. The Operational Commander must think of "hostile act," "hostile intent," and "lethal fires" in a new environment, that of the electronic attack against ideals, and must propose to the Strategic level of command a rationale for departing from existing State practice. This paper gives some thoughts in those regards, reviewing existing law, examining potential future threats and means for further investigating them, and then setting out a good-faith basis for modification or extension of existing law.

`

> "We are now in the midst of a revolution in military affairs unlike any seen since the Napoleonic Age . . . an information revolution that enables a shift from what we call platform-centric warfare to Network-Centric Warfare."[1]

With those words, VADM Arthur K. Cebrowski, President of the Naval War College, introduced a volume of scholarly discussions of many of the legal "jus in bello" aspects of information warfare. While the discussion of the application of international humanitarian law is useful, it still leaves the Operational Commander wondering just when it is appropriate to use military means to address the challenges of information operations. As new threats emerge, as new technologies are adapted to cause us harm, as the nature of the adversary changes, the traditional ways of thinking about armed conflict – massed armies of "privileged combatants"[2] against massed armies of "privileged combatants" – must undergo a metamorphosis.

DRAWING NEW LINES IN THE COLORING BOOK

As technology advances and non-state actors take the fore as a threat to the United States, our thinking as to what constitutes a threat and what warrants a self-defensive response must likewise evolve. International law continually plays a game of catch-up due to its very nature: treaties and other international agreements take years to negotiate and conclude, and entry-into-force adds additional time;[3] customary international law is established by State practice, and it simply takes time to determine what that practice is. This field of State practice lends itself, then, to innovative approaches, and it is the duty

[1] Arthur K. Cebrowski, "CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 2.

[2] This term is a shorthand for those belligerents who meet the requirements of the Geneva Convention to qualify as prisoners of war: they carry arms openly; they wear fixed, distinctive insignia; they are under the command of a responsible commander; and they operate in accordance with the law of armed conflict.

[3] An example is the United Nations Convention on the Law of the Sea, opened for signature in 1982 and entered into force in 1994.

of the Operational Commander to lay the groundwork for innovative approaches to technological threats. The Operational Commander is in the "bully pulpit" when it comes to advancing the thinking in this field. Cooperation among the various Commanders at the operational level – U.S. Special Operations Command (USSOCOM); U.S. Joint Forces Command (USJFCOM); U.S. Strategic Command (USSTRATCOM) in particular – will be crucial to these future advances.

Employing military force in defense of national interests is somewhat like coloring in a coloring book. Some people are disciplined, but unimaginative, and so keep their coloring within the prescribed lines. Others may have great imaginations, but they have not harnessed their energies, and therefore are all over the page. The former group receives praise from the adults for having the picture "look right." The latter group endures the overwrought sighs of disapproval.

There is a third group, one that is not so often appreciated, and that is the group that knows how to move the lines so that the coloring is all within them. They are the true visionaries. They must take the new missions – SOCOM with its focus on terrorism, for example, where the asymmetry represented by cyber attack is significant – adapt the old techniques – application of force in response to a hostile act or demonstration of hostile intent – and advance the thinking.

The Operational Commander looking into the twenty-first century must be prepared to propose and develop new definitions, new ways of looking at old problems. The Operational Commander needs to assist the Strategic level of command in advancing these ideas so that, in time, they become customary international law. The lines in the coloring book must be changed.

WHERE WE ARE AND WHY IT IS LACKING

Information warfare is an area where definitions and doctrine lag far behind. Two areas in particular – defining hostile act and intent, and understanding lethality – are ripe for investigation and development.

> The requirement of an armed attack as a condition of legitimate self defense, in accordance with Article 51, precludes not only threats. Recourse to self-defense under the Article is not vindicated by any violation of international law short of an armed attack. Even declarations of war, if it is evident to all that they are unaccompanied by deeds, are not enough. The notion that mere mobilization or 'bellicose utterances' as such may justify self-defense within the framework of Article 51, has no foundation.[4]

Professor Dinstein's formulation was certainly correct in the age of kinetic warfare, where nations employed weapons against each others' armed forces and infrastructure, and sometimes (probably illegally) against each others' populations, to compel an enemy to bend to their will. The question now, though, is whether the understanding of "armed attack" goes far enough; this is the point that the Operational Commander must press.

Over the course of the last one hundred years, and especially since the adoption of the United Nations Charter, nations have been careful to couch many of their uses of military force in terms of self-defense. The national philosophies have been translated into the doctrine of military commanders, whose guidance to their forces on the use of force frequently requires identification of a "hostile act" or the divination of "hostile intent" before weapons may be released.[5] Yesterday's punch in the nose, however, may become tomorrow's subtle electronic intrusion, which is why "hostile act" must be

[4] Yoram Dinstein, *War, Aggression and Self-Defense* (Cambridge, England: Cambridge University Press 1994, 2d Edition), 184.
[5] *See, e.g.*, CJCSI 3120.1A of 15 Jan 2002, Standing Rules of Engagement for U.S. Forces, ¶ 5a.

redefined. Likewise, Operational Commanders are wedded to the definition of "lethal fires" as those that cause death or injury to persons, or destruction of things.[6] In the future, however, the idea of the death of an ideal should be included within the notion of "lethal fires" lest certain threats go unaddressed. As will be discussed in more detail below, there is more to a State than its borders and its people, and attacks against those intangible aspects – national philosophy, quality of life – can "kill" the State just as effectively as attacks against persons can kill persons.

Further complicating the problem is the likelihood that persons employing the technological attack will not act as "privileged combatants" – that is, they will not regard the strictures placed upon nation states in the decision to go to war or in the conduct of that war. When deciding how to react to these unprincipled combatants, the Operational Commander must be careful to observe the targeting restraints of the law of armed conflict. In a contest where the proper reaction could spell the difference between national "life" and national "death," the understanding of the threat and the international restraints are particularly important; the Operational Commander must understand proportionality, target discrimination, and necessity in new terms.

Most of the literature to this point has discussed the kinetic effects of computerized network attacks: for example, the effects that are unleashed if a dam control system is tampered with, or the effects if air traffic control is interrupted. The scholars all seem to agree that those sorts of effects can constitute an "armed attack" for purposes of invoking the inherent right of self-defense.[7] Where the scholars' efforts fall

[6] *See* Milan Vego, *Operational Warfare*,(Newport, RI: Naval War College Joint Military Operations Department 2000), 240.

[7] *Compare* Daniel B. Silver, "Computer Network Attack as a Use of Force under Article 2(4)," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law

short is in focusing on the self-defense right in a vacuum – more properly, perhaps, the United Nations charter should be read as a whole, and greater attention should be focused on earlier articles. This approach will lead the Combatant Commander to propose definitions of hostile act and hostile intent that depart from current practice, but the very real threats to both American society and the international community demand these departures.

PRESENT SHOCK

This approach is not based on mere fantasy, either. Many, if not most, readers of this paper can recall instances when internet services were disrupted by some sort of malicious event such as the introduction of the Sasser virus. Corporations such as McAfee, Symantec, and EMCC make fortunes designing file-protection and file-storage systems. The world has shrunk considerably because of electronic connections, and one perhaps unintended consequence is that all persons, and all governments, are increasingly at risk:

> Even as the threat of great power war diminished, we remained focused largely on state-versus-state conflict. [The need to transform the military] is a by-product of the effects of globalization in the international security order as well as the transition from the industrial age to the information age. We have the emergence of the phenomenon which we call the systems perturbation.[8]

The United States has recognized this threat for some time. "Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of

Studies, vol. 76, 2002), 73,82-83, *with* Horace B. Robertson, Jr., "Self-Defense against Computer Network Attack," also in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 121, 132-33. Robertson comes close to recognizing the point of this paper that nonkinetic attacks can be viewed as a use of force in certain cases.

significantly harming both our military power and our economy."[9] The Decision cited forms a useful basis for Operational Commanders to investigate the weaknesses and compensating for them. It also forms a useful basis for establishing a new State practice.

> The United States relies for its very existence--economically, socially, and politically--on an extraordinary sophisticated and intricate set of long-distance networks for energy distribution, communication, and transportation. Because these networks also rely upon each other, a truly serious disruption in any one will cascade quickly through the others, rending the vital fabric of our nation at its most crucial points. Under these circumstances, the ability to respond to national security crises will at least be severely constrained and may be completely interrupted for some crucial interval. Thus, in addition to their serious vulnerabilities to accidents and nature, these networks present a tempting target to terrorists and to any antagonist contemplating an international move contrary to U.S. interests.[10]

Kluepfel's observation, affirmed by the Presidential Decision Document and by the writings of scholars discussed throughout this paper, gives urgency to the task of viewing the problem of computer attack through a "new" lens.

Where the Operational Commander truly becomes involved is in defining what constitutes a "hostile act" or what constitutes "hostile intent" that will give rise to self-defensive actions. It is not enough now to look at a "punch in the nose" as the triggering event, as punches in the nose now come in different forms. Instead, the technological threat should be seen in different ways.

NATIONS AS HUMANS

[8] U.S. Congress. Senate. Committee on Armed Services. *Emerging Threats and Capabilities: Hearing before the Senate Armed Services Committee* on S. 1050, 108th Cong, 1st Sess. 2003. Testimony of VADM (Ret.) Arthur K. Cebrowski, Director, Office of Defense Transformation, 18, 20.

[9] Presidential Decision Document 63 of 22 May 1998. Because this document is not readily available from traditional sources (e.g., Volume 3 of the Code of Federal Regulations), it is included as an Appendix.

[10] Hank Kluepfel, "Countering Non-Lethal Information Warfare," AFCEA ARGENTINA, <http://www.afcea.org.ar/publicaciones/kluepfel.htm>, no publication date provided, viewed 15 May 2004. Note that Kluepfel, while talking about the political and economic threats, considers this aspect of information warfare "non-lethal".

To tackle this problem of “hostile act” and “hostile intent” in the technological age, one must first think of nations more as humans. The Charter of the United Nations is a starting point for the Operational Commander’s consideration of the issue: Article 2(4) prohibits the “threat or use of force” against the “territorial integrity and political independence” of member states. It further prohibits other threats or uses of force that are inconsistent with the purposes of the Charter, whose preamble calls upon all nations to employ international machinery for the promotion of the economic and social advancement of all peoples. [11]

In approaching nations as humans, it is useful to consider what constitutes a “State” under international law, primarily because it is the States that are the focus of most international agreements. The Operational Commander who moves away from the abstraction of “State” and concentrates on the attributes of “State” may have an easier time of articulating what, technologically, can constitute a threat to the State’s “life.”

In the modern international system, a State is a person with attributes of “personhood” like those of human persons in domestic legal systems – status in the system, rights and obligations before the law, power to acquire and own property, to make contracts, to assert legal claims, to pursue legal remedies.[12] A State is seen, internationally, as the legal equal of every other State. In the United Nations General Assembly, for example, each nation has one vote. “As applied to a State, elements long identified with ‘sovereignty’ are inevitably only metaphors, fictions, fictions upon fictions; some of them, however, do constitute essential characteristics and indicia of Statehood today. I consider these to include principally: independence, equality,

[11] Charter of the United Nations, 1945.
[12] Louis Henkin, “General Course on Public International Law,” *Recueil des Cours* 216 (1989): 28.

autonomy, 'personhood,' territorial authority, integrity and inviolability, impermeability, and 'privacy.'"[13] Those "metaphors, fictions, and fictions upon fictions" are the same for a State as one's personality, one's temperament, one's control over one's body and destiny are for a human being, and threats to that metaphorical state of being should be viewed identically to a threat against a human being.

> From princes and the law of princes, States inherited also the integrity and inviolability of their territorial domain, and exclusive authority within it. For purposes of relations with other countries, the prince's country was both domain and home, in which he had complete authority as well as title. Other princes did not legitimately exercise authority in a prince's territory or have relations with his subjects. In the modern international State system, too, the State has complete authority in its territory and over persons, activities and things within it.[14]

It should be but a small step in logic to conclude that anything which interferes with that State's authority can constitute a threat to that State's "life," just as an insurrection against the Prince could cost the human Prince his life. A threat to the way a State conducts its political process, for example, or to the livelihood of a State, should be the concern of the future warfighter.

The difficulty with current Rules of Engagement and their definitions is that, too often, they focus on the effects on persons and things, and not the effect on an ideal. The current unclassified definition of hostile act, for example, is "an attack or other use of force against the United States, US forces, and, in certain circumstances, US nationals, their property, US commercial assets, and/or other designated non-US forces, foreign nationals and their property."[15] These Rules of Engagement, moreover, are written

[13] *Ibid*.
[14] *Ibid*.
[15] CJCSI 3121.01A of 15 Jan 2000 ¶ 5g.

against the backdrop of title 10 of the United States Code,[16] which defines the United States only in the geographical sense.[17] This same shortcoming – a focus on persons and things, not ideals – appears in the definition of "lethal fires". Until Operational Commanders are given the tools that they need – broader definitions that more correctly encompass the threat – the United States is vulnerable to a non-traditional attack. A proposed new definition of "hostile act" is included as an Appendix in an effort to frame the thinking on this topic.

This non-traditional attack is the potent threat of the future. It is likely not an "armed attack" or "armed aggression" as that term was understood when the Charter was adopted, as the capability did not then exist,[18] but as will be demonstrated it is more than mere "bellicose utterances".[19] What, exactly, is the Operational Commander responding to in the case of a non-traditional attack on abstraction, and how does he frame his response? Recent history provides an example.

INTEREFERENCE WITH THE POLITICAL PROCESS

One recent example of possible interference with the political process in violation of Article 2(4) of the Charter has a kinetic component. In March 2004, a bomb or several bombs were detonated during rush hour in Madrid. Hundreds were killed, more were injured. In national elections that coincidentally were held several days later, the Aznar government that had supported the United States' position in the war against Saddam

[16] This portion of the United States Code represents the Congressional exercise of power conferred in Article I of the U.S. Constitution to raise and support armies and to provide and maintain a Navy. U.S. Const. Art. I § 8 cl. 12-13.
[17] 10 U.S.C. § 101.
[18] *See, e.g.*, Louise Doswald-Beck, "Some Thoughts on Computer Network Attack and the International Law of Armed Conflict," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 164-65.
[19] Dinstein, 184.

Hussein was voted out and replaced by a government that pledged to remove Spanish troops from Iraq.

The Spanish case may be an obvious one of how a terrorist act – bombing commuter trains – can influence the political process, although investigators (notably Judge Baltazar Garzon) have not finished their work. A less obvious case could occur outside the view of the international community, but its effect would be no less real.

That "less obvious case" could occur in the United States. In the wake of the presidential election confusion in 2000, the United States set about trying to improve its system of recording its citizens' votes. Because our system is federal, each state and territory is responsible for its own mechanical conduct of elections – some states have "bubble-in" ballots, for example; some have the infamous "butterfly ballots" with its attendant problem of "hanging chads". One cannot forget the media coverage of the armed convoy that escorted paper ballots to Tallahassee, Florida, in late November/early December 2000; the outcome of the examination of the ballots would determine the political direction of the United States for the following four years. It is entirely possible, too, that the outcome of that election did determine the course of international events.

Some states are now investigating electronic means of voting as a hedge against future such controversies. "People are just realizing exactly what we've brought into some states," said State Senator Andrew Harris of Maryland, a Republican. "The stakes are so high. I don't put it above someone trying to manipulate elections on a grand scale."[20] To echo that legislator's concern, one can imagine a case where a hotly contested state in a national election has its electronic election data corrupted; if the corruption is undetected before the state's chief election official certifies the results, then the corrupter of the data has succeeded in changing the self-determination of the residents.

In fact, for the damage to occur, the manipulation need not be on even so grand a scale as a nationwide election. Imagine a closely contested Senatorial race, for example. For the last five Congresses,[21] the difference between the majority party and the minority party has been razor-thin. As many key functions of our federal Government depend on Senate action (for example, advice and consent to Executive appointments; advice and consent to treaties; advice and consent to Judicial appointments), the difference between majority and minority takes on added significance. Likewise is the case of legislation, which must, of course, clear both Houses of Congress before it may be enacted. If even one of the thirty-three biennial Senate elections is corrupted, that can have an impact.

One can also consider other statewide elections,[22] these for Governor. Our federal system depends on some cooperation between state and federal governments, especially in the war against terrorism. A Governor hostile toward the federal government's policies could easily stymie efforts to fight terrorism, either by not cooperating with the Department of Homeland Security or NORTHCOM, or by not allowing National Guard troops to be readily pressed into service. [23] Because the "hook" in most cases is simply federal money (the federal government will give states money in return for cooperation;

[20] Robert Tanner, "States Seek Backup for Digital Voting," Boston *Sunday Globe*, April 4, 2004, A17.

[21] A "Congress" is a term of art and refers to a two-year period beginning on January 3 of odd-numbered years when all members of the House of Representatives are sworn into new two-year terms; one-third of the members of the Senate are sworn into new six-year terms.

[22] Because Senators represent an entire state, and not just a district of a state, their elections, unlike those for Representative in Congress, are considered statewide.

[23] There are cases where the National Guard can be placed into federal service over the objection of a state governor, as was demonstrated in Little Rock, Arkansas, in the era of desegregation, when President Eisenhower overrode Governor Orval Faubus' direction not to enroll black students in formerly all-white schools, but that case is an extreme example.

they withhold it in the absence of cooperation), one or two renegade governors (however unlikely the prospect from a domestic politics standpoint) can cause great harm.

While the likelihood of interference may be unlikely at present, the capabilities to interfere with the political process through electronic means exist, and the President recognizes that they exist; the National Strategy for Homeland Security includes "information systems" within its areas of concern. .[24] This is exactly the sort of threat to "political independence" and "territorial integrity" that the United Nations Charter contemplates, although through a different medium from 60 years ago.[25] It is important, then, for the Operational Commanders to begin seeing these attempts at manipulation for what they are, namely, lethal fires. If the fires are effective, their target, a government, a way of life, can be destroyed. Viewing these attempts to influence the political process as threats to the nation's "life" will lead to a better assessment of the threat and a better process for responding to the threat. It will assist the Operational Commander in proposing newer definitions to respond to newer threats.

The challenge for the Operational Commander is to take that concern and translate it into action.[26] Commander, JFCOM, for example, exercising his training function, could develop the factual backdrop against which interference could occur; Commander, STRATCOM, could add expertise on detection of interference and determination of its source; Commander, SOCOM, could devise the response in the non-conventional arena.

[24] George W. Bush, *The National Strategy for Homeland Security*, 16 July 2002, xi.

[25] On a strategic level, it may also be viewed as a violation of the Charter's prohibition on any other acts that are inconsistent with the purposes of the Charter (international economic well-being, for example).

AFFECTING THE SENSE OF "DOMESTIC TRANQUILITY"

Another important intangible, non-kinetic, effect, of an electronic intrusion is the loss of the sense of "domestic tranquility" which is one of the cornerstones of our nation's founding.[27] As one example, the Massachusetts legislature is considering tracking dangerous parolees with a Global Positioning System transponder.[28] If an adversary wanted to disrupt social affairs, that would be a prime target. Likewise, an adversary could manipulate the GPS to rearrange a nation's internal borders, causing upheaval in the economic sector when tax revenues for the various states are adjusted, or disrupting the myriad commercial transactions that now depend on GPS time.[29]

Scholars recognize this non-kinetic effect in trying to reach the virgin territory of hostile attack in the 21st century.

> Significant human physical or mental suffering is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise comprises damage or destruction . . . . As an example, a major disruption of the stock market or banking system might effectively collapse the economy and result in widespread unemployment, hunger, mental anguish, etc., a reality tragically demonstrated during the Depression of the 1930's."[30]

Schmitt's concern is echoed by another author, this one writing not of the legal aspects of the threat and responses but rather of the engineering aspects:

> Of more concern is the presence of a technically feasible 'strategic' threat. That is, the means exist to cause significant damage and disruption to U.S. public and private information assets, processes, and systems . . . . Such

[26] *See, e.g.*, the charge in the Unified Command Plan of 30 April 2002, ¶ 11a, to "deter[] attacks against the United States . . . ."

[27] U.S. Const. preamble.

[28] Ralph Ranalli, "Bill Seeks GPS to track offenders," Boston *Globe*, Thursday, 13 April 2004, B2.

[29] *See generally* Bob Brewin, "GPS Jammers Raise Concern," *Computerworld* on-line (January 20, 2003), available at http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C77702%2C00.html, most recently viewed ,14 May 2004>. The technology is discussed generally in Dawn Stover's article, "New War in Space," *Popular Science*,

[30] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and the *Jus in Bello*," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 187, 194.

> an attack, or the threat of such an attack, could thwart our foreign policy objectives, degrade military performance, result in significant economic loss, and perhaps even undermine the confidence of our citizens in the Government's ability to protect its citizens and interests.[31]

Alberts' "strategic" threat translates to new missions, and new challenges, for the Operational Commander:

> National infrastructures have come under increasingly intense scrutiny in recent years as potential targets for information attack. A Presidential Commission identified eight infrastructures that must be protected from the depredations of information and other kinds of attack. These were: electrical power, gas and oil (storage and transportation), telecommunications, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government services.[32]

Those infrastructures ensure not only this nation's ability to respond to disasters but our very standard of living.

This threat to "Domestic Tranquility" has been the focus of several studies in the recent past. As one example, shortly after the United States suffered the terrorist attacks in 2001, the Naval War College devised a war game to see just how devastating a cyber attack on the United States could be. Dubbed "Digital Pearl Harbor," this game considered the effect on critical infrastructure of attacks in the financial, power, and internet sectors. The study concluded that attacks on the various sectors were survivable, but that serious degradation in the quality of American life would occur. The summary of the game, and the organizers' conclusions, are provided as an Appendix.

[31] David S. Alberts, *Defensive Information Warfare* (Washington, DC: National Defense University 1996), 13.

[32] Roger W. Barnett, "A Different Kettle of Fish: Computer Network Attack," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 21, 31. The "Presidential Commission" to which Barnett refers produced the outline for the Presidential Decision Document cited in footnote 9 above.

Another, ongoing, effort is that of the Sandia National Laboratory's Information Design Assurance Red Team ("IDART"). This program focuses on the malevolent intent of adversaries then provides techniques, tools, research and training that can be employed to make systems more secure. Teams conduct three types of investigations. A targeted vulnerability analysis of information systems examines how information is used, stored and transmitted in operational, prototype, administrative, supervisory control and data acquisition systems, as well as in hybrid setups typically used in critical infrastructure.[33]

Both the Digital Pearl Harbor study and the IDART represent tools that the Operational Commander should employ in examining and understanding the new threat. The IDART technique is particularly useful for mining that most difficult of ores, the "hostile intent" that may give rise to the use of force in self-defense.[34] These resources demonstrate that the threats are not imaginary but can cause real damage to the United States the abstraction, not only the United States the physical entity.

CONCLUDING THOUGHTS

In the context of international military operations, international law sets the boundaries within which one must color. Although the drafters of Article 51 may not have anticipated its use in protecting States from destructive actions perpetrated through technological means, international law has long recognized the need for flexible application.[35] Threats to political independence and territorial integrity, or for that matter uses of force inconsistent with any of the purposes of the United Nations, that involve the subtle force of electronics must be put on the agenda of every Operational Commander.

[33] "Information Systems See Red," *Signal*, February 2004), 47-48.
[34] *See* Robertson, 121-22.

"Determining the moment when a State may legally take armed defensive action as a matter of self-preservation is difficult enough in the arena of conventional armed attack . . . [b]ut when an attack . . . can be initiated without warning and instantaneously by a few computer strokes or clicks of a mouse at a location remote from the target State, determining the threshold criteria is even more difficult."[36] Those who determine the "threshold criteria" are the Operational Commanders – for example, STRATCOM with its mandate to operate in the "ethereal" world; SOCOM with its mandate to defeat non-conventional threats – and it is they who will bear the burden of advancing the thinking in the near term.

The approving or disapproving audience comprises both sovereign nations and the populations of those nations. Commanders who keep their operations within the appropriate boundaries generally accomplish their missions while avoiding international disapproval. Commanders who scribble outside the lines frequently fail in their missions, and often run afoul of international norms in the process.

The visionaries are those Commanders who are willing to recognize changed circumstances and to push for changes in the way the international community regards

[35] James P. Terry, "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 421, 425.

[36] Horace B. Robertson, Jr., "Self-Defense against Computer Network Attack under International Law," in *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002), 121, 121-22.

their actions. The future of this nation, of this civilization, depends on their willingness and courage to move the lines in the coloring book.

`

BIBLIOGRAPHY

SYMPOSIUM: *Computer Attack and International Law* (Newport, RI: Naval War College Press International Law Studies, vol. 76, 2002)

Individual authors and articles:

Barnett, Roger W. "A Different Kettle of Fish: Computer Network Attack"
Cebrowski, Arthur K. "CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers"
Doswald-Beck, Louise. "Some Thoughts on Computer Network Attack and the International Law of Armed Conflict"
Robertson, Horace B., Jr. "Self-Defense against Computer Network Attack"
Schmitt, Michael N. "Wired Warfare: Computer Network Attack and the *Jus in Bello.*"
Silver, Daniel B. "Computer Network Attack as a Use of Force under Article 2(4)"
Terry, James P. "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?"

BOOKS:

Academie de Droit Internationale. *Recueil des Cours* 216. Dordrecht, Netherlands: Martinus Nijhoff Publishers, 1990.
Alberts, David S. *Defensive Information Warfare.* Washington, DC: National Defense University, 1996.
Dinstein, Yoram. *War, Aggression and Self-Defense, 2d Edition.* Cambridge, England: Cambridge University Press, 1994.
Vego, Milan. *Operational Warfare*. Newport, RI: Naval War College Joint Military Operations Department, 2000.

TREATIES AND INTERNATIONAL MATERIALS:

Charter of the United Nations, 1945
Protocol Additional I to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 1125 U.N.T.S. 3, 1977.

CONSTITUTIONS, STATUTES, AND CONGRESSIONAL MATERIALS:

U.S. Constitution
U.S. Code
U.S. Congress. Senate. Committee on Armed Services. *Emerging Threats and Capabilities: Hearing before the Senate Armed Services Committee* on S. 1050, 108th Cong, 1st Sess. 2003

EXECUTIVE BRANCH MATERIALS:

Bush, George W. *The National Strategy for Homeland Security*, 16 July 2002
CJCSI 3120.1A of 15 Jan 2002, Standing Rules of Engagement for U.S. Forces
Presidential Decision Document 63 of 22 May 1998
Unified Command Plan of 30 April 2002

PRINT PERIODICALS:

Stover, Dawn. "New War in Space." *Popular Science*
"Information Systems See Red." *Signal*, February 2004.

ELECTRONIC SOURCES:

Brewin, Bob. "GPS Jammers Raise Concern." *Computerworld* on-line, January 20, 2003. Available at <http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C77702%2C00.html>.
Kluepfel, Hank. "Countering Non-Lethal Information Warfare." *AFCEA ARGENTIA*, no publication date provided. Available at <http://www.afcea.org.ar/publicaciones/kluepfel.htm>.

APPENDIX A

FOR OFFICIAL USE ONLY

THE WHITE HOUSE
WASHINGTON

May 22, 1998

PRESIDENTIAL DECISION DIRECTIVE/NSC-63

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF VETERANS AFFAIRS
ADMINISTRATOR, ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
THE ASSIST TO THE PRESIDENT FOR
NATIONAL SECURITY AFFAIRS
THE ASSISTANT TO PRESIDENT FOR
SCIENCE AND TECHNOLOGY
THE CHAIRMAN, JOINT CHIEFS OF STAFF
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: Critical Infrastructure Protection

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non- traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services.
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector or counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, I want those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.
- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.
- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.
- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, providing information upon which choices can be made by the private sector. These incentives, along with other action, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.
- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be

available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.
- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.
- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.
- We must focus on preventive measure as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.
- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and action shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. <u>Structure and Organization</u>

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. <u>Lead Agencies for Sector Liaison</u>: For each infrastructure sector that could be a target for significant cyber or physical attack, there will be a single U.S. Government department which will serve as the lead agency for liaison. Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Protection Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. <u>Lead Agencies for Special Functions</u>: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of

Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by me and report to me through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, I will appoint a panel of major infrastructure providers and state and local government officials to serve as my National Infrastructure Assurance Council. I will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to me as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorities to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorities.

No later than 180 days from the issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to me a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines, for implementation, responsibilities and funding.

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

4. Response: We shall develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

6. Education and Awareness: There shall be Vulnerability Awareness and Education Program within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to me as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to me and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI	Law enforcement and internal security

CIA	Foreign intelligence
State	Foreign affairs
Defense	National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to me through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison officials and Special Function Coordinators shall attend the CIGC's meetings. Departments and agencies shall each appoint to the CIGC a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, I immediately authorize the FBI to expand its current organization to a full scale National Infrastructure

Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, I also direct the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of international threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIP will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies

(DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government,. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly it extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. it would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used be the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.
- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.
- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.

- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.
- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.
- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.
- The National Academy of Science and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.
- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.
- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

Internal Federal Government Actions

APPENDIX A

In order for the Federal Government to improve its infrastructure security these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.

- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.

- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.

- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.

- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.

- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

- GSA shall identify large procurements (such as the new Federal Telecommunications System ETS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Review Act strategic planning and performance measurement framework.

- The NSA, in accordance with its National Manager responsibilities in NSD 42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

Assisting the Private Sector

In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.

- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.

- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways to deterring and responding to computer crime by juveniles.

[signed:] Bill Clinton

APPENDIX B

“Hostile Act” means an attack or other use of force, kinetic or non-kinetic, against the United States, its system of Government, its political subdivisions, their system of Government, US forces, and, in certain circumstances, US nationals, their property, US commercial assets, the US economy or critical infrastructure, and/or other designated non-US forces, foreign nationals and their property.

One example of “hostile act” includes an attempt to corrupt the data used to determine elections. Another example includes an attempt to corrupt the data necessary to transmit commercial information.

Actors against whom self-defensive actions may be taken may include individuals, organizations, or nation-states.

APPENDIX C

Seminar Game Concept, Design, and Analysis

Game Concept

Purpose

To determine and design the most damaging attack to the U.S. delivered largely or completely through cyber means. The cyber attack is the means, not end result of the game; it was more important to damage the U.S. using the internet than to damage the Internet itself. Vulnerabilities are viewed from terrorist point of view.

The most important result is to get specific enemy courses of action so the feasibility of enemy attacks (and of a "Digital Pearl Harbor" size of result), interactions across industries, and the effectiveness of current countermeasures can be judged.

Why Multiple Industries?

Attacking multiple industries is likely to cause greater devastation than just attacking one sector alone, and would make efforts to recover from an attack more difficult. In addition, exploration and examination of the complexities faced by the enemy in a multi-industry attack, and differences across industries in coping with an attack, can lead to a broader range of insights and provide a more comprehensive understanding of the issue.

Why the Selected Industries?

Electrical Power was deemed vital to the vast majority of productive activities in the modern economy. Communications are important in themselves and as a facilitator for post-attack recovery. The Communications industry was divided into Telecommunications and the INTERNET in order to investigate the close relationship between the two. The Finance sector was deemed a likely target, is a major component of U.S. economic (and even symbolic) power, and is the one example of a distributed industry in the set.

What is the Threat?

The game designers wanted a recognizable opponent. The opponent is a non-state actor that has access to state intelligence, is well informed, and has significant resources. Taking the opposite approach and using a nation-state as the opponent ran the risk of distracting players into considerations of post attack self defense, alternative national policies, *et cetera*.

Why Game This?

To apply planning process to all steps necessary to conduct attack. The steps considered are: Strategic Planning, Preparation, Initial Attack, and Continuing Attacks/Counter-recovery.

General

Digital Pearl Harbor was played as a single-sided seminar-style game where a given scenario was examined in four phases, or moves. The exercise covered two days of game play and consisted of facilitated discussion moderated and facilitated by Gartner, Inc. and Naval War College staff members, respectively. The participants were provided scenario briefs at the beginning of each exercise day, and were subsequently divided into specific groups to plan for and respond to the challenges that such a scenario might involve. Each group was directed to select a spokesperson to present a summary of the group's discussions in plenary sessions convened at the end of each phase.

Phase I: Strategic Planning and Preparation

An initial brief and Phase I were conducted during the first day of the exercise. In this phase the individual industries members analyzed the situation and identified the strategic goals for their industry. They also analyzed the support and logistic requirements needed to plan for and prepare a credible attack given the confines and limitations of the scenario.

During this and the next two phases, the Red Commander's Cell provided strategic coordination and guide lines that ensured the industry plans were synchronized for maximum damage and effect. With coordination from the Red Commander's Cell, each industry planned attacks that were essentially self-supporting (with the significant exception that the Internet cell provided much help to others), but the did not rely on detailed coordination to create maximum effect. Red Cell's outbriefs for Phase I, II, and, III are located in Appendix C, Appendix D, and Appendix E, respectively.

Phases II through IV: Attacks

Phases II through IV were conducted from the beginning of the second day through the morning of the last day of the exercise. In Phases II and III, each industry developed progressively more detailed and specific attack plans designed for each industry. Following Phase III, plenary session members and REDCOM noted that many attack plans relied on methods that required perfect execution and significant human infiltration of infrastructure, and thus possessed numerous single points of failure. Taking this into account, phase IV tasked the industry cells to identify those critical planning elements that did not have work arounds, and/or to develop alternate attack plans.

Issues, Insights and Observations

Major Insights

As a single event, Digital Pearl Harbor cannot provide definitive answers to the results all types or methods of attack developed during the exercise. However, by the end of the exercise widespread agreement was achieved that a cyber attack was indeed possible and was most devastating when attacks were coordinated and planned together. Individually, many of the attacks alone would cause some isolated damage, but taken together could possibly cause widespread panic or at a minimum a loss of confidence with the government to protect the citizens from the damage cause by a cyber attack.

Electrical Power

This cell designed a joint physical-cyber attack centering on the destruction of physical transmission bottlenecks and corruption of the supervisory control and data acquisition (SCADA) systems which allocate power across lines. (This exact plan of attack has been discussed in the open literature.) The multitude SCADA programming companies (a within the game, within the cell internet search revealed approximately 7000) makes it simple to acquire of SCADA software for testing purposes, or even to write and sell SCADA software with pre-designed back doors. However, this very multitude of SCADA programmers creates a multitude of idiosyncratic programs, making it very difficult to know how to hack into large numbers of them. "War dialing" (i.e. sending out a barrage of candidate passwords to gain access) would help gain access to the SCADA systems. (That this might create an observed pattern of hacking that would alert authorities seems not to have been discussed.) However, some SCADAs are not physically connected to the Internet, and numerous physical backups are available. The cell concluded that control of the power grid through control of the SCADA systems was likely to last no more than 15 minutes.

If this is the worst damage that cyber attackers could inflict by attacking the electrical power system, then the country is relatively safe from this avenue of attack, and one should not lightly dismiss the modesty of this group of attack designers. The combination of "air gaps" (i.e. SCADAs that are physically disconnected from the Internet, either at all times or can be disconnected by an operator as a result of obvious meddling from a source on the Internet), and the diversity of SCADA software, do indeed add significantly to the security of the power grid. Moreover, the synergy of the physical and cyber attacks means that the physical attack is vital, and such attacks are more difficult in reality than they ever seem in the design phase. (Otherwise, eco-terrorists among others would have accomplished many such attacks long ago.)

In private communications after the DPH game, 2 separate players (who were among the more knowledgeable people on these matters) said that the threat to the SCADAs was underestimated. Attacks with longer effects were possible, security was lax in the extreme, and the diversity of code in different SCADAs did not prevent hackers from gaining control in at least 1 exercise within a matter of minutes. Permanent destruction of the SCADA software was considered feasible, requiring a major reprogramming effort and/or replacement of hardware. The threat level expressed by the game output may well represent a lower bound to the real threat, and further investigation is clearly warranted.

Electrical Power Group outbriefs for Phase I, II, III, and, IV are located in Appendix F, Appendix G, Appendix H, and Appendix I, respectively.

Financial Services

The stated goal for each game cell (representing 1 of the 4 industries listed above) was to disrupt and/or destroy their target industry in order to affect a crisis of confidence in the United States. No group took the phrase "crisis of confidence" or the concept of FUD (fear, uncertainty, doubt) more seriously than the financial services cell. This cell designed attacks involving the infiltration of personnel into legitimate banks and/or buying banks and having a few powerful personnel within them work the plot. Most plots involved creating legitimate-looking transactions that could pass for real ones for a few days. The cell planned to sabotage millions of individual checking accounts with these bogus transactions. Only when checks started bouncing or when end-of-month statements revealed zero or negative balances would most of these victims know. This, *when executed just before a massive cyber attack that destroyed current records and backups for many banks* (arranged by the Internet cell), would put numerous consumers in the position of being unable to buy groceries, pay household bills, et cetera. This was intended to cause maximum FUD. A second aspect of the plan was the sabotage of the payroll and bank clearing house systems, again arranged through the Internet cell. The planned date for this was chosen to maximize the number of affected people by interfering with both the receipt of paychecks and major shopping days.

Many aspects of this plot were cyber only in that "wire transfers" of money count as cyber and the fact that the Internet cell's plan to destroy records and backups was cyber. Much of what was plotted could be done by anyone with control of a seemingly legitimate bank, so long as they did not plan to transfer the money to themselves and stay within U.S. jurisdiction or an extradition zone to spend it. While computers would make it easier to compile credit card numbers for further fraud, a small pool of labor and a lot of advanced preparation would probably be adequate to accomplish a smaller but similar crime without it having any cyber aspect. Therefore, it may not constitute a new threat in the same sense as, say, offshore control of computers running physical hardware, for instance. Furthermore, it seems close enough to money-making plots to raise the question of why we have not seen this before. Surely, the argument runs, many criminals would take advantage of such a method of getting money (drug lords are known to own several banks) and then transfer it outside the reach of U.S. authority. This point is countered with the argument that money is only useful to criminals if they can continue to draw from a functional banking system, and it is the subsequent destruction of the banking system by the Internet saboteurs that makes it the plan work in the long run. Therefore, there is no real way to make money from this plan, so the failure of criminals to conduct such a crime/attack is *not* evidence that it is infeasible. This counter-argument is debatable since small-scale uses of the same tactics would seem to allow criminals to steal significant sums of money and use cyber attacks to destroy the evidence of criminal means in attaining these sums. These questions remain unresolved.

Perhaps the greatest criticism of this cyber attack is that it does not reach a level of damage appropriate to the label of "Digital Pearl Harbor." If millions of households had their financial records scrambled to their great disadvantage and were unable to pay for "the necessities," the effect would be not unlike a natural disaster that wipes out some of their wealth. In such circumstances, the government steps in and arranges for critical services to sustain the victims. If millions of families could not pay their water bills, the government could and probably would order the water companies to supply water at a nominal cost, subsidize the companies, and/or loan/give money to the victims. This is exactly what happens in flood- and earthquake- related disasters. While this is costly and in some small way reduces the incentive to earn and save money and to insure against this type of disaster, it seems to be at most a minor impediment to the efficient functioning of our economy. Adverse incentives have been present for those who build on floodplains for many decades, and floods have repeatedly destroyed the assets of people there, yet the impact cannot be said to equal Pearl Harbor.

Financial Group outbriefs for Phase I, II, III, and, IV are located in Appendix J, Appendix K, Appendix L, and Appendix M, respectively.

The Internet

The plan conceived by the Internet cell was the most massive of all the plans developed. Indeed, the Internet cell's plan was so all-encompassing that they offered their services to the other cells!

This cell's plan revolved around the insertion of malicious code into many machines. The malicious component of this code would be activated by a specific signal; until such activation, the code would perform some useful function, both to cover its true purpose and to make it more popular. Given away as freeware, it might allow the infection of millions of machines, thus allowing their control when the signal was given. To accomplish this, the cell planned to buy a software company (perhaps a security consulting company!) and/or an Internet service provider (ISP), most of whose employees would have no idea of the plot in which they were assisting. Over time, this company would probe for access paths to computers on the web in a way that was indistinguishable from normal hacking. Simultaneously, it would identify software vulnerabilities in other products and design viruses and worms for attacking them. (The details of this attack are very similar to those given in the article "How to Own the Internet in Your Spare Time.")

The best method of propagating this software on the Internet was considered to be a malicious peer to peer (P2P) or shareware program. Such code is already written into software used by the now-defunct Napster.com and the currently operating KaZaA.com. It allows for the control of one machine by another, for transfer of audio files in the cases listed above, and for any other purpose the shareware designer wishes.

On signal, the Trojan Horse software embedded within the freeware application would tunnel in through the previously located vulnerabilities in others' software, install itself on millions of machines, and then release storms of bogus messages for a distributed denial of service (DDOS) attack and/or erase data and software on the infected machine, at the control of the plotters.

The Internet cell was so confident of their ability to control the Internet and connected networks by this means that they planned a series of massive DDOS attacks before their attacks on the other cells' industries, leading up to a finale in which they crash the Internet itself, and keep it from functioning in the face of (national?) efforts to resurrect it. In fact, the cell considered that they could "seize the Internet" after 1 year of spreading their software. Moreover, some of the cell members in subsequent private communications have announced that they have devised even more insidious and therefore undetectable plans to accomplish the same ends. In short, the cell viewed the Internet as easy to destroy and/or use to destroy other industries.

Internet Group outbriefs for Phase I, II, III, and, IV are located in Appendix N, Appendix O, Appendix P, and Appendix Q, respectively.

Telecommunications

This cell designed qualitatively different attacks for disruption and destruction. The disruptive attacks proposed were 1) disruption of the atomic clocks and/or global positioning system (GPS) used to synchronize message sending/receipt, 2) insertion of malicious code through upgrades and the telecommunication industry's use of open source software, and 3) exploiting the SS7 network (which is designed without security as the network itself is assumed to be secure). There was great debate within the cell about how easy it is to hack into the SS7 network. The best method found for getting inside the system was buying a small telephone system, preferably overseas. For disruptions, the following table was made:

Vulnerability	Impact	Execution
Timing Sources	High	Difficult
Signaling Network	High	Moderate
Outside Facilities	Low to High	Easy to Moderate
Software	High	Easy to Moderate
Data Bases	Low	Difficult
OSS	High	Moderate to Difficult
Protocols	High	Easy to Difficult

The destructive attacks devised by the telecommunications cell were largely if not exclusively physical rather than cyber. The main proposed attacks consisted of cutting the 3 undersea fiber-optic cables connecting the U.S. to other continents (from NYC, Miami, and San Luis Obispo) and destroying the 5 primary switching centers ("peering centers") for domestic traffic. The 3 undersea cables and the 5 switching centers have well known locations, most of which were explicitly discussed within the cell. Undersea cables were to be cut by a device dragged by a fishing trawler or by SEAL-like divers. Buildings with peering centers could be destroyed by truck bombs, or the relevant floors full of equipment destroyed by teams entering during a fire or chem/bio alarm, which itself could be triggered by a Trojan horse program in a PROM (programmable read only memory). In addition, cables could be destroyed or rendered useless by flooding, which could be caused by a single operator with a backhoe; 5 such attacks were planned.

With the exception of the plan to drag cable-cutting devices from trawlers, the plans for *destroying* the telecommunications network seemed to rely less on untested assumptions than the plans created by the other groups.[37] Exact

[37] The plans for disruption, involving logic bombs and sleeper code, were so closely analogous to the plans of the Internet cell that their feasibility is probably identical to the feasibility of the Internet cell's plan. (The specifics of cyber-disruption of the atomic clocks were judged to be more difficult than other components

knowledge of the routes of cables and their underground passageways would be required. While approximate locations are available on the Internet, exact locations may require some quite literal footwork, but this is not demanding, nor is it likely to reveal the plot. Operating backhoes in the middle of streets might attract some unfavorable notice, but if the attackers were clever enough to dress in workmen's clothing, it seems unlikely that someone would actually call the relevant authorities to verify the legitimacy of the operation, and the plot would stand a good chance of success. However, as soon as such plots started to have effects across the country, the pattern would be instantly recognized. It also requires a relatively large number of people to execute, and many of them would not be expected to escape.

The trawler/cable-cutter plan seems fraught with uncertainties. A large, ground-penetrating plow designed to be a cable-cutter bears a very close resemblance to an anchor, and pulling one through several feet of sand might require much more of a ship than can be inconspicuously bought or rented by a group from outside the few industries that operate such large vessels. An alternative plan of training and using underwater demolitions personnel was suggested, but the difficulties of countries in using trained professional "frogmen" in wartime to accomplish similar missions indicates that this is perhaps not very likely to succeed.

Telecommunications Group outbriefs for Phase I, II, III, and, IV are located in Appendix R, Appendix S, Appendix T, and Appendix U, respectively.

of the plan; their physical destruction was then offered as a simpler alternative.) The one significant difference lies in the accessibility of necessary specific information about the software, which is far more widespread for the Internet than it is for telecommunications. For other aspects of such plans, please refer to the Internet section for details.

Conclusion

All industries except the Internet itself seem to have significant vulnerability to attack, but *probably* not to the extent of creating (singly or in combination) a Digital Pearl Harbor. The governmental mechanisms for dealing with shocks to peoples' incomes and to the banking sector would prevent a wider disaster from following the designed attacks on banks and individual's accounts within them. By contrast, the designed attack on the telecommunications industry would be disastrous, but that attack required an enormous amount of physical intervention to succeed. Even if such plots fall within the definition of a *Digital* Pearl Harbor, their physical components seem too large to be plausibly executed without warning. The attack on the power grid stands alone as an example of modesty; even the cell members did not consider their attack to be a Pearl Harbor -- with the very significant qualification that individuals with great knowledge subsequently told me of far greater threats that had not been examined by the cell. (This alone motivated the word *probably* in this paragraph's opening sentence.)

The Internet cell told a different story; if their designed attack is credible, there is a genuine threat of disaster from cyber attack. Moreover, the cell seemed constrained by the pace of the game and the discretion of the players from devising even more damaging attacks, which players have subsequently offered to discuss in a more secure setting. The only consolation was that they admitted that "90 percent" of their attack could be defeated by the use of *currently recommended* security practices.